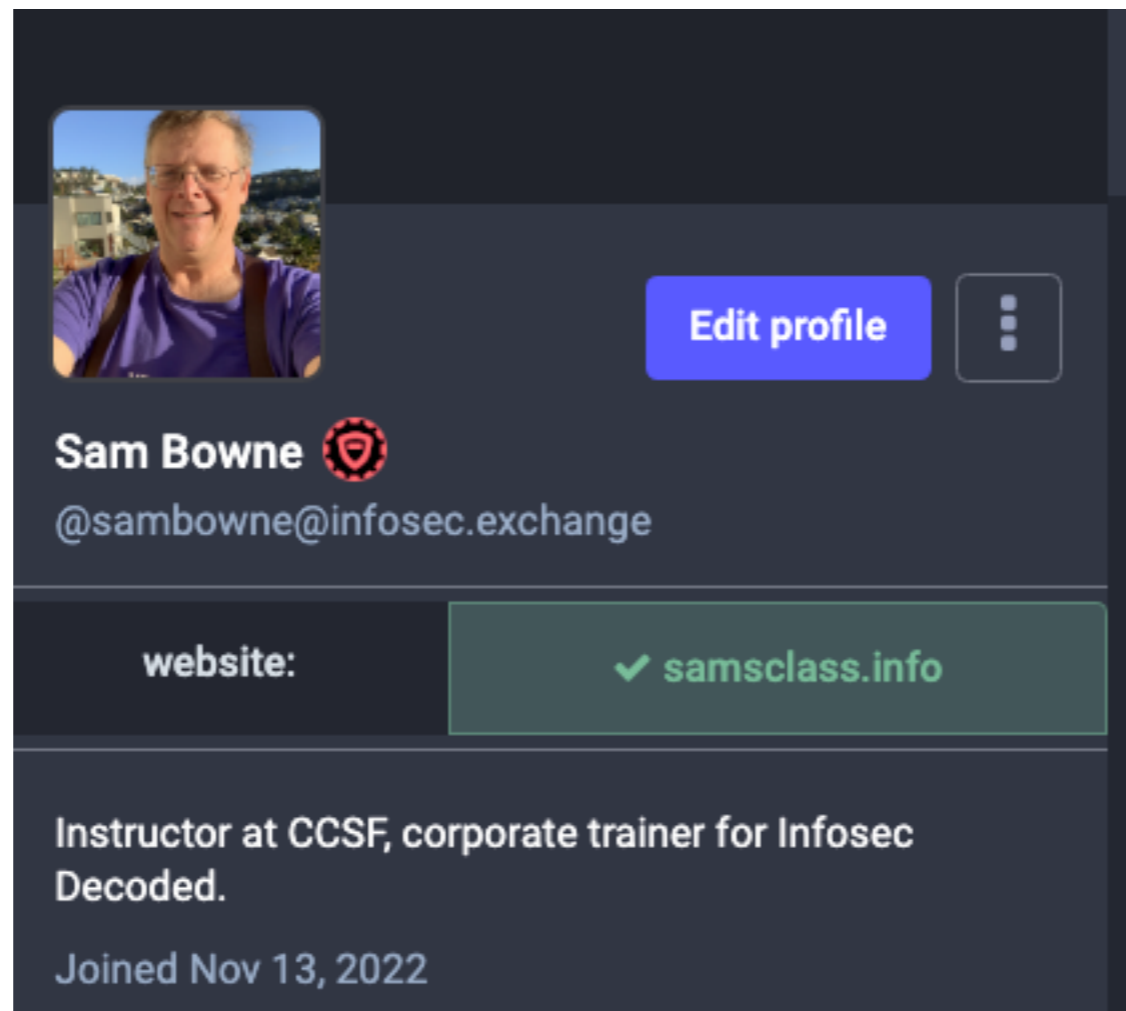


Cyberwar


Updated 8-16-23

Mastodon


- infosec.exchange



A screenshot of a Mastodon profile page for Sam Bowne. The profile includes a profile picture of a man with glasses and a purple shirt, a blue 'Edit profile' button, and a three-dot menu icon. The name 'Sam Bowne' is displayed with a red shield icon, and the handle '@sambowne@infosec.exchange' is shown below. A 'website:' field contains the link 'samsclass.info' with a green checkmark. The bio reads 'Instructor at CCSF, corporate trainer for Infosec Decoded.' and the join date is 'Joined Nov 13, 2022'.



[Edit profile](#)

Sam Bowne 

@sambowne@infosec.exchange

website: [✓ samsclass.info](https://samsclass.info)

Instructor at CCSF, corporate trainer for Infosec Decoded.

Joined Nov 13, 2022



Official Blog

Insights from Googlers into our products, technology, and the Google culture

A new approach to China

January 12, 2010

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two

China cyberattack

US firm Mandiant has issued a 74-page report on a global cyber espionage campaign by what it says is a Chinese government-backed organization dubbed APT1 (Advanced Persistent Threat 1)

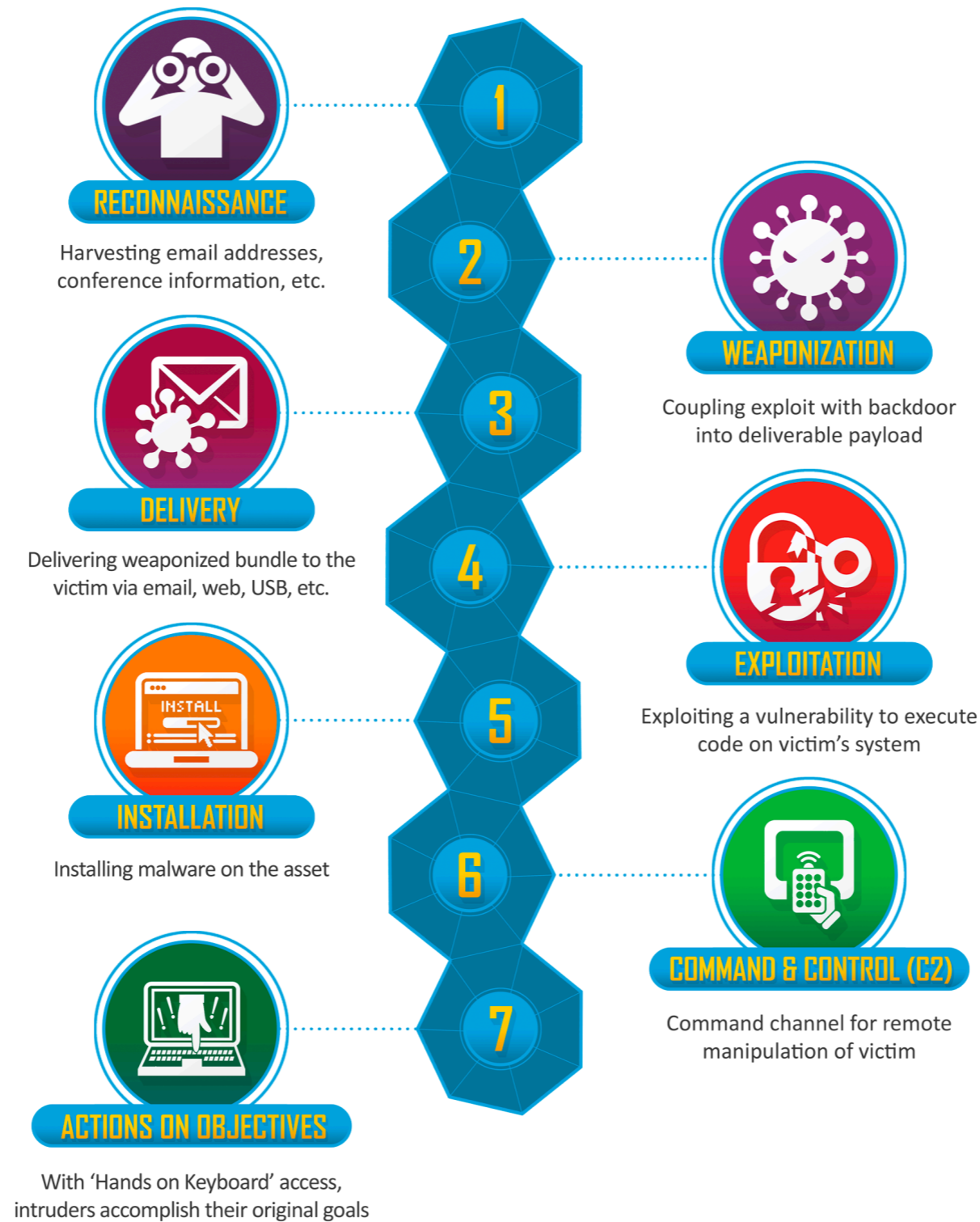
APT1 global attacks since 2006

141 organizations targeted
in 15 countries



- <https://www.rfa.org/english/news/china/hacking-02222013121848.html>

Lockheed-Martin Kill Chain



Mitre ATT&CK

The screenshot shows the MITRE ATT&CK website interface. The browser address bar displays 'attack.mitre.org/tactics/enterprise/'. The navigation menu includes 'Matrices', 'Tactics', 'Techniques', 'Data Sources', 'Mitigations', 'Groups', 'Software', 'Campaigns', 'Resources', and 'Blog'. A search bar is located in the top right of the navigation area. The left sidebar lists various tactic categories: Enterprise (selected), Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Mobile, and ICS. The main content area is titled 'Enterprise tactics' and includes a breadcrumb trail 'Home > Tactics > Enterprise'. Below the title is a descriptive paragraph: 'Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.' To the right of this text, it states 'Enterprise Tactics: 14'. A table lists 14 tactics with their IDs, names, and descriptions.

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

APT groups [edit]

American advanced persistent threat groups [edit]

- [Equation Group](#)^[28]

Chinese advanced persistent threat groups [edit]

- [PLA Unit 61398](#) (also known as APT1)
- [PLA Unit 61486](#) (also known as APT2)
- [Buckeye](#) (also known as APT3)^[29]
- [Red Apollo](#) (also known as APT10)
- [PLA Unit 78020](#) (also known as APT 30)
- [Periscope Group](#) (also known as APT40)

Iranian advanced persistent threat groups [edit]

- [Elfin Team](#) (also known as APT33)
- [Helix Kitten](#) (also known as APT34)

North Korean advanced persistent threat groups [edit]

- [Reaper Group](#) (also known as APT37)
- [Lazarus Group](#) (also known as APT38)

Russian advanced persistent threat groups [edit]

- [Fancy Bear](#) (also known as APT28)
- [Cozy Bear](#) (also known as APT29)

The biggest cybersecurity threats to the US



RUSSIA

America's most sophisticated cyber adversary.

Notable attack:

The plot to interfere in the 2016 US presidential election by the Internet Research Agency.



IRAN

There has been significant uptick in cyber attacks in recent years.

Notable attack:

Iranian Behzad Mesri charged with hacking into HBO, leaking "Game of Thrones" scripts and demanding \$6 million in ransom.



CHINA

Once launched noisy attacks, but is now more subtle.

Notable attack:

Chinese military officers stole secrets on fighter jets, including the F-35, from Lockheed Martin.



NORTH KOREA

High on US watchlist despite better diplomatic relations.

Notable attack:

The US blamed North Korea for the WannaCry attack in 2017.

Insider Inc.

CISA

- Cybersecurity & Infrastructure Security Agency
- <https://www.cisa.gov>
- Jen Easterly,
Director



Nation-State Cyber Threats

APT groups are often nation-state actors or state-sponsored groups. CISA regularly publishes alerts and advisories to help defend against state-sponsored malicious cyber activity. See the following webpages for overviews of publicly available, open-source intelligence and information regarding state-sponsored cyber threats from four nations: [China](#), [Russia](#), [North Korea](#), and [Iran](#).



- <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors>

Chinese Attacks

- *"China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."*

Russia

- *"Recent Russian state-sponsored activity has included destructive malware and ransomware operations. Prioritizing patching of known exploited vulnerabilities is key to strengthening operational resilience against this threat."*

Iranian Attacks

- *"Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."*
- *<https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran>*

North Korea

“North Korea’s cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat... [and] continues to adapt to global trends in cybercrime by conducting cryptocurrency heists...”

US Attack Tools

STUXNET, THE WORLD'S FIRST DIGITAL WEAPON



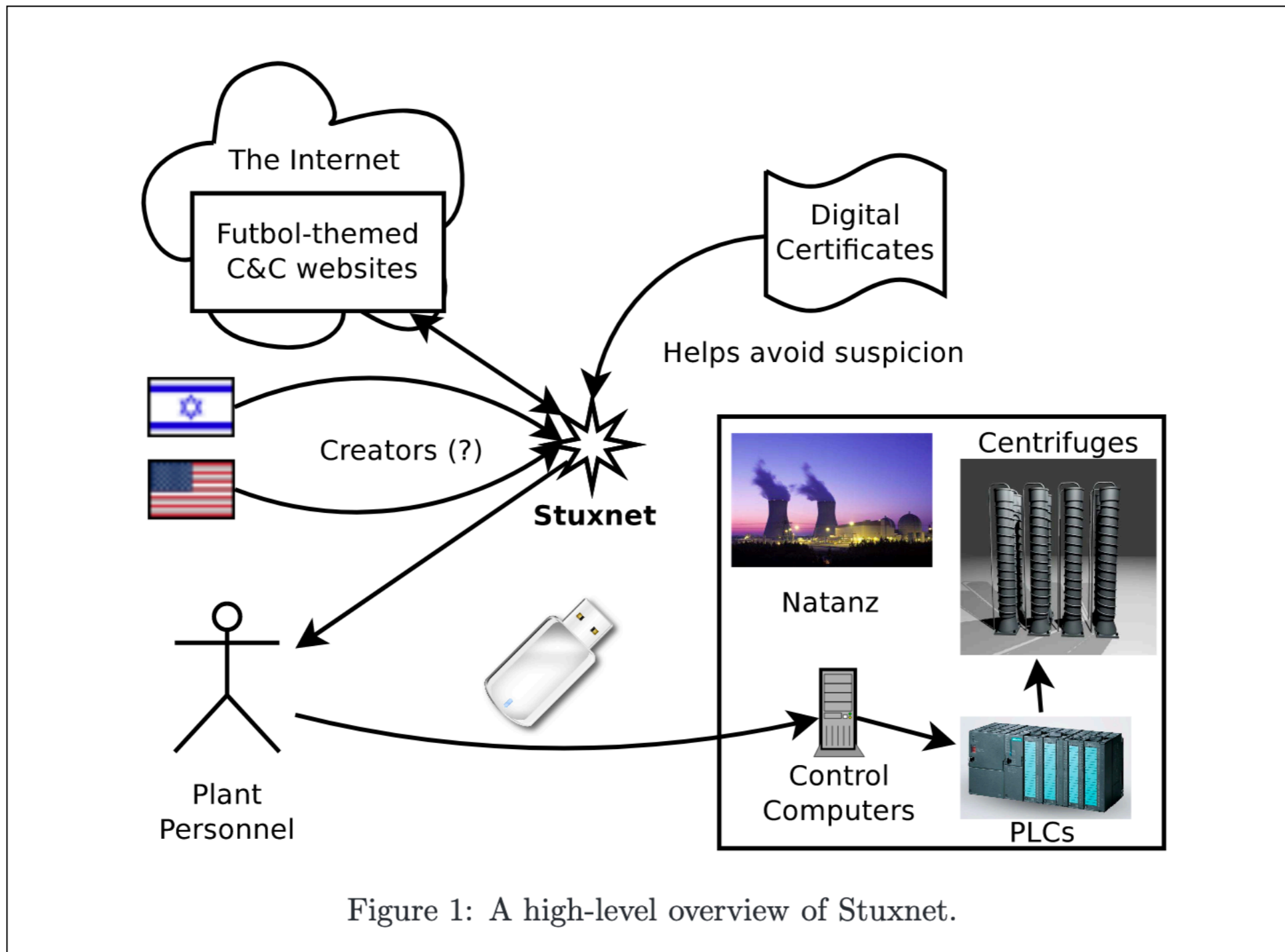
Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008.  OFFICE OF THE PRESIDENCY OF THE ISLAMIC REPUBLIC OF IRAN



This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.

 AP PHOTO/SPACE IMAGING/INTA SPACETURK, HD

<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>



<https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>

2.3 Command and Control servers

After Stuxnet establishes itself on a computer, it tries to contact one of two servers via HTTP:

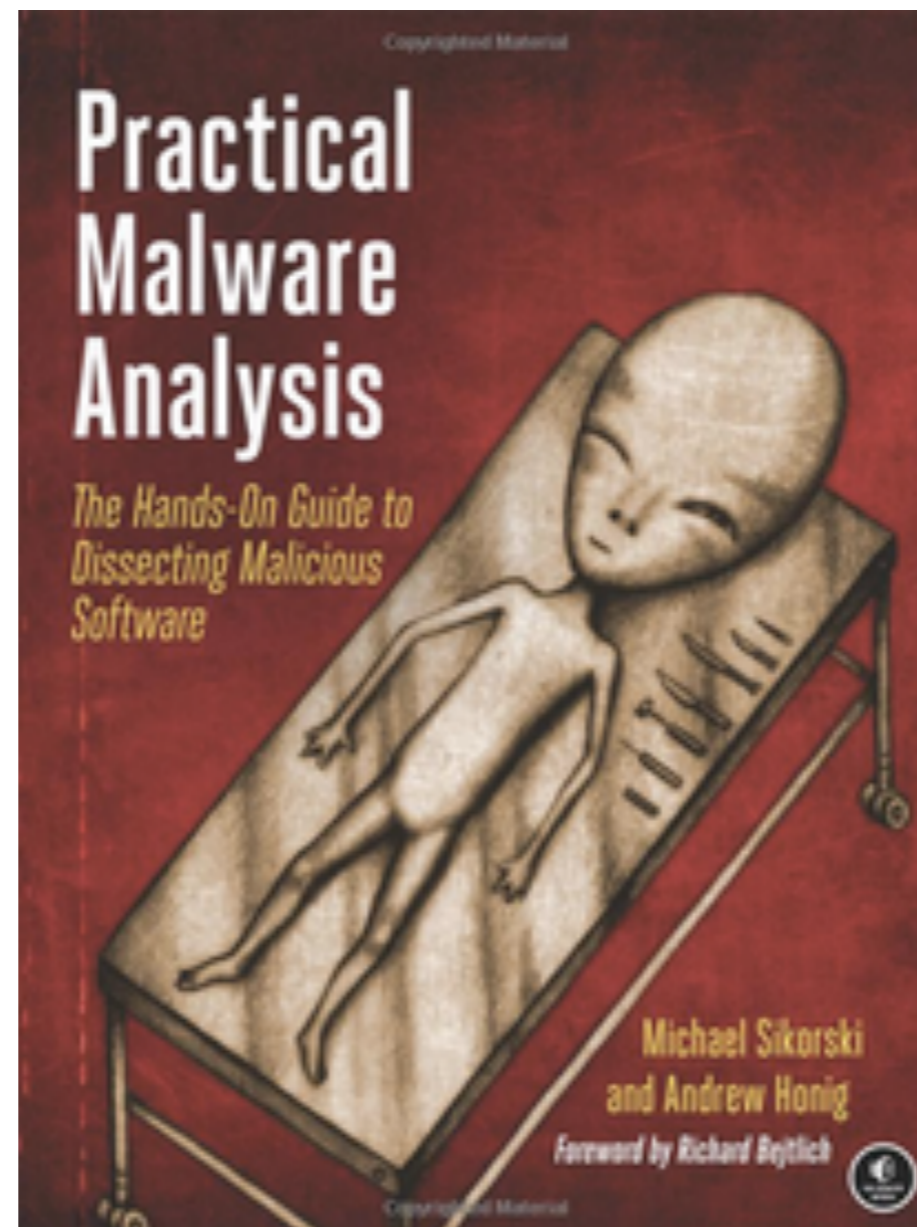
- www.mypremierfutbol.com
- www.todaysfutbol.com

2.4.2 Kernel-Mode

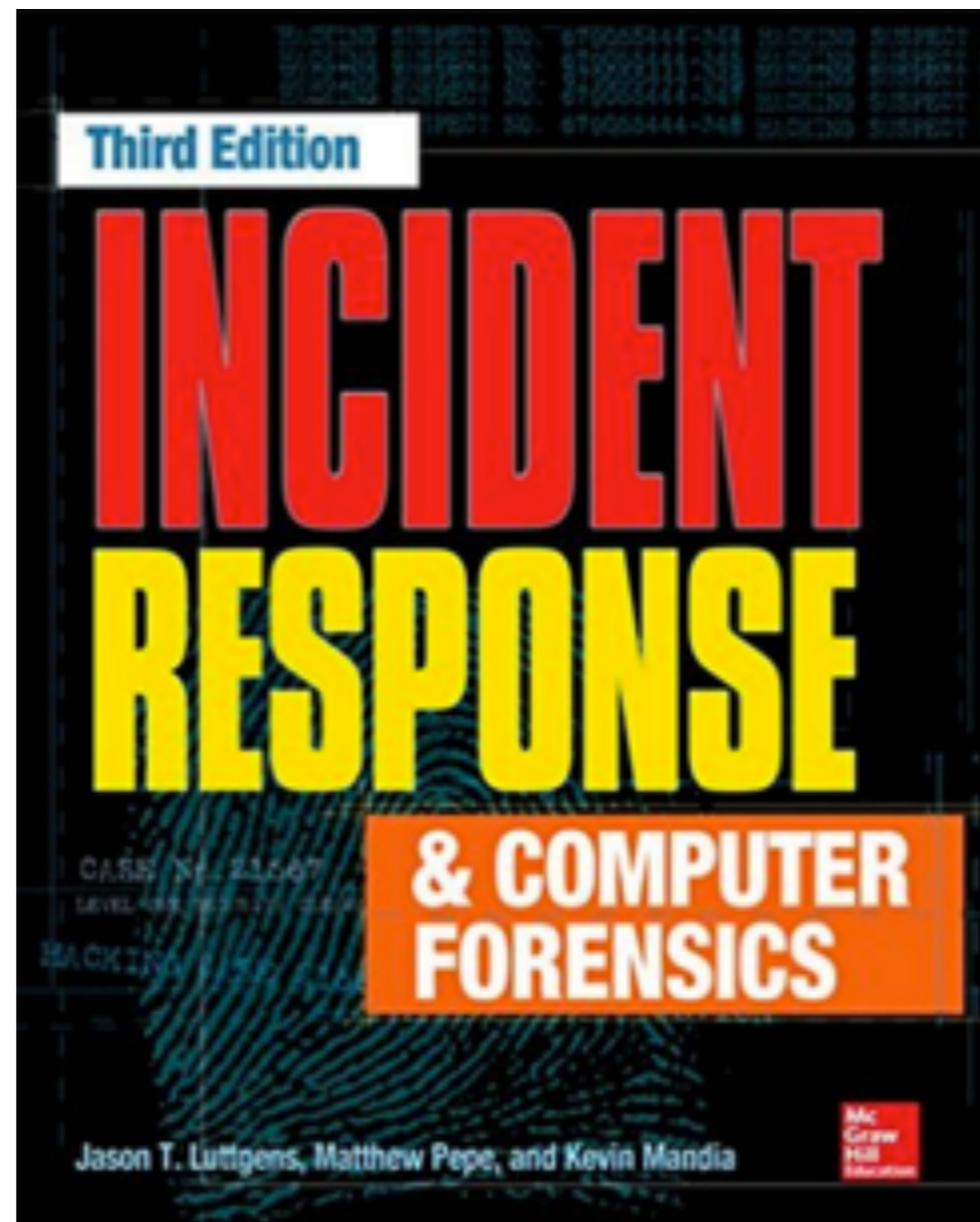
Stuxnet installs two kernel-mode drivers. `Mrxcls.sys` is a driver signed by a Realtek certificate as shown in Figure 6. When Stuxnet wants to install it onto the system, it marks it as a boot startup so it starts in the early stages of Windows boot. This driver first reads a registry key which has been written in the installation step and contains the information for injecting Stuxnet images into certain processes.

The other driver, `Mrxnet.sys`, is actually the rootkit and is also digitally signed by a Realtek certificate. It creates a device object and attaches it to the system's device objects so that it can monitor all requests sent to these objects. The purpose of this job is to hide files which meet certain criteria from users.

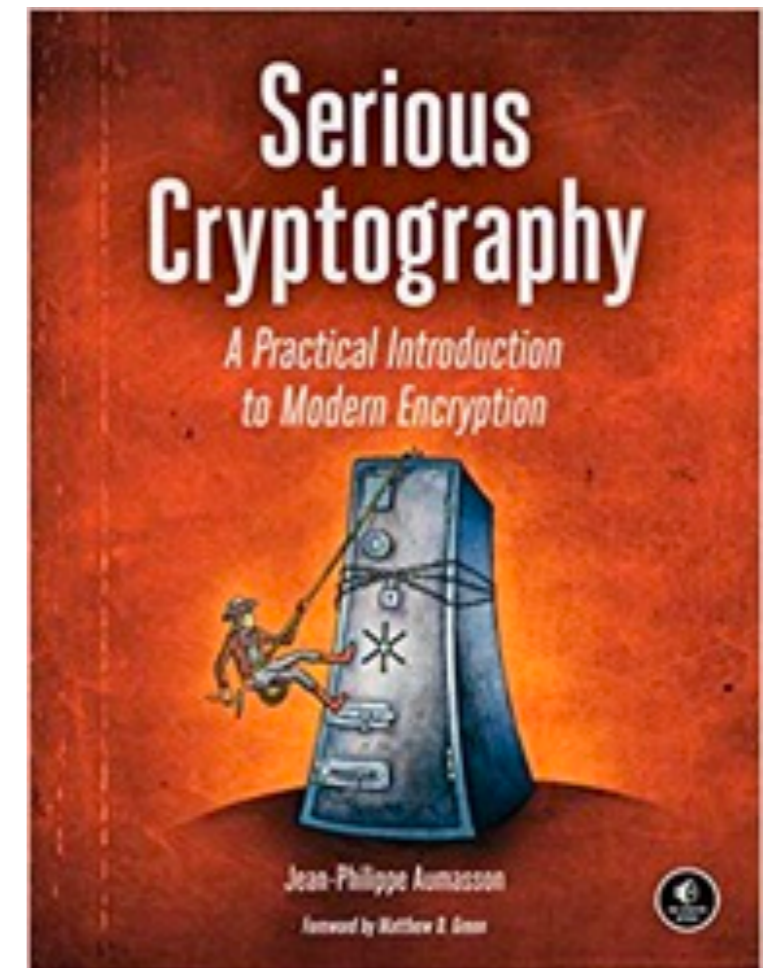
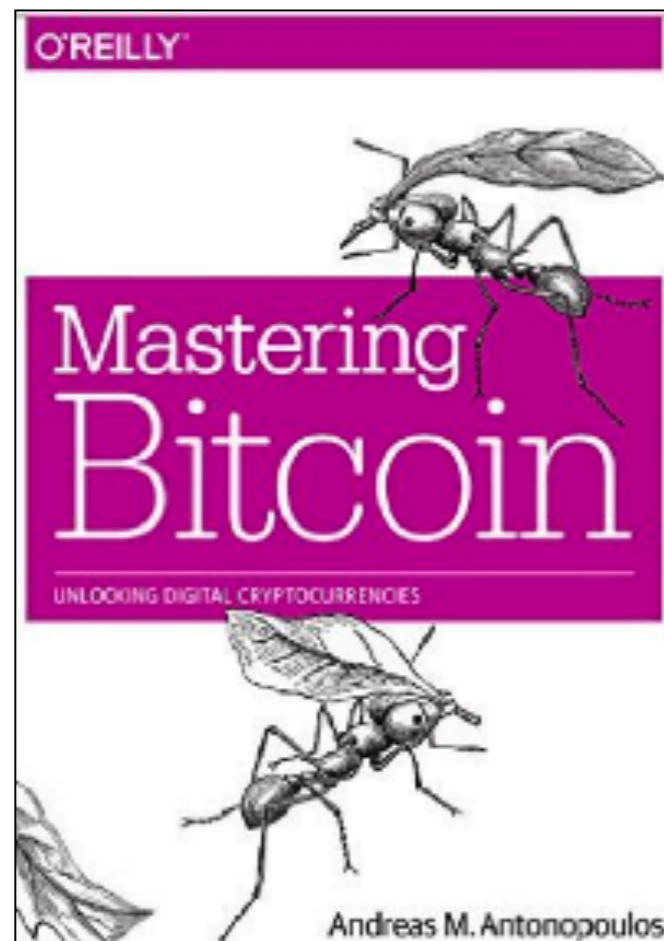
CNIT 126: Practical Malware Analysis



CNIT 152: Incident Response



CNIT 141: Cryptography for Computer Networks



Kahoot!

1c